Vehicle Infrastructure Integration (VII)

Network Subsystem Specification (SSS)

Research and Innovative Technology Administration

April 20, 2007
Version 1.1

Booz | Allen | Hamilton

This report is confidential and intended solely for the use and information of the company to whom it is addressed.

Acceptance / Approval Page

// //____ Reviewed by ________________________
David Cline Date
Quality Assurance

// //____ Reviewed by ________________________
Mark Lawrence Date
Deputy Project Manager

// //____ Approved by ________________________
Craig Pickering Date
Project Manager

// //____ Approved by ________________________
Bill Jones Date
US Department of Transportation

DOCUMENT CHANGE HISTORY

Date	Author	Description
12/06/2006	Booz Allen Hamilton	1.0 Released.
4/20/2007	Booz Allen Hamilton	Version 1.1 Section 1.2 (Document Overview) has been amended to remove the reference to Appendix D (Lexicon). The *VII Infrastructure Lexicon* is now a separate document. Subsection 1.2.1 (Requirements Language) has been rewritten to refer to *VII Infrastructure Lexicon* as a separate document. Figures 2-1, 2-2 and 2-3 have been revised to delineate the boundary between the VII System and external entities. Section 2.1 (System Overview) has been revised for better clarity. The definition of the Network Access Point (NAP) has been moved to the beginning of Section 2.1. The term "Infrastructure Servers" has been defined. Section 2.2 (VII Infrastructure) has been added, along with Figure 2-4, to define the VII Infrastructure and clarify the correlation between the Network Subsystem, the VII Infrastructure, the VII System and external entities. In Figures 2-2, 2-3 and 2-5 through 2-8, the word "Gateway" has been added to clarify that the four gateways described in these diagrams are inside the NAP, and an icon representing the NAP servers has been added. The narrative section on Communications Services (now Section 2.4) has been expanded to describe Classes of Service and DNS Service in greater detail. In Section 4.2, new Communications Services requirements have been added. Requirement NTWK25, listed in Section 4.4 in the previous release of this document, has been deprecated and replaced with more specific requirements listed in Section 4.2. In Appendix B (Reference Documents), titles and version numbers of the documents have been updated. In addition, the documents listed in this appendix have been grouped by topic for easier reference. Appendix C has been renamed to National System Requirements Traceability. Appendix C has been updated to include traceability of all newly added Communications Services requirements and to exclude requirement NTWK25, which has been deprecated. Throughout the document, all references to *National System Specification* have been replaced with references to *National System Requirements* and all references to NSS have been replaced with references to NSR.

Table of Contents

1 INTRODUCTION

This Subsystem Specification (SSS) is based on guidance and information provided by the USDOT, subsequent meetings and discussions, and agreed upon assumptions by the USDOT and VIIC. Every effort has been made to ensure the content and approach in developing this document reflects available guidance from the USDOT and accurately reflects the overall scope and intent of the Vehicle Infrastructure Integration's (VII) objectives.

1.1 SCOPE

This document, the *VII Network Subsystem Specification*, addresses the functional and facilities requirements for the Network Subsystem. This specification is the first of a series of technical documents detailing the Network Subsystem and defining the technical characteristics of the VII System. The main focus of this document is the Proof of Concept (POC) system functionality, which will subsequently be implemented in the National System. For further background on the VII System's projected operations, refer to the *VII National System Requirements* (Reference 1) and the *VII Concept of Operations* (Reference 2).

1.2 DOCUMENT OVERVIEW

This SSS captures the comprehensive system requirements for the Network Subsystem as part of the VII project. The remaining SSS sections are organized as follows:

- **Section 2. Network Subsystem Description:** Describes the Network Subsystem in the context of the overall VII System. Provides details on the four major network transport interfaces and their corresponding gateways inside the Service Delivery Node (SDN) Subsystem.
- **Section 3. General Network Requirements:** Specifies high-level requirements that apply to the entire VII infrastructure. (None have been identified in this version of the document.)
- **Section 4. Functional Requirements:** Specifies all functional Network Subsystem requirements, including requirements for the communications services, connectivity between VII nodes, protocols to be used in network communications, classes of service, network management, security, and time.
- **Section 5. Performance Requirements:** Specifies requirements related to the scalability and reliability of the VII Network Subsystem. (Specification of these requirements is left to a future release of this document.)
- **Section 6. Facilities Requirements:** Specifies requirements related to the facilities that will house Network Devices and Security Devices.
- **Appendix A: Assumptions and Dependencies:** Provides a list of the assumptions and dependencies related to the requirements.
- **Appendix B: Reference Documents:** Provides a list of reference documents related to the Network Subsystem.
- **Appendix C: National System Requirements Traceability:** Traces requirements from this document to their parent requirements in the *VII National System Requirements*.

1.2.1 Requirements Language

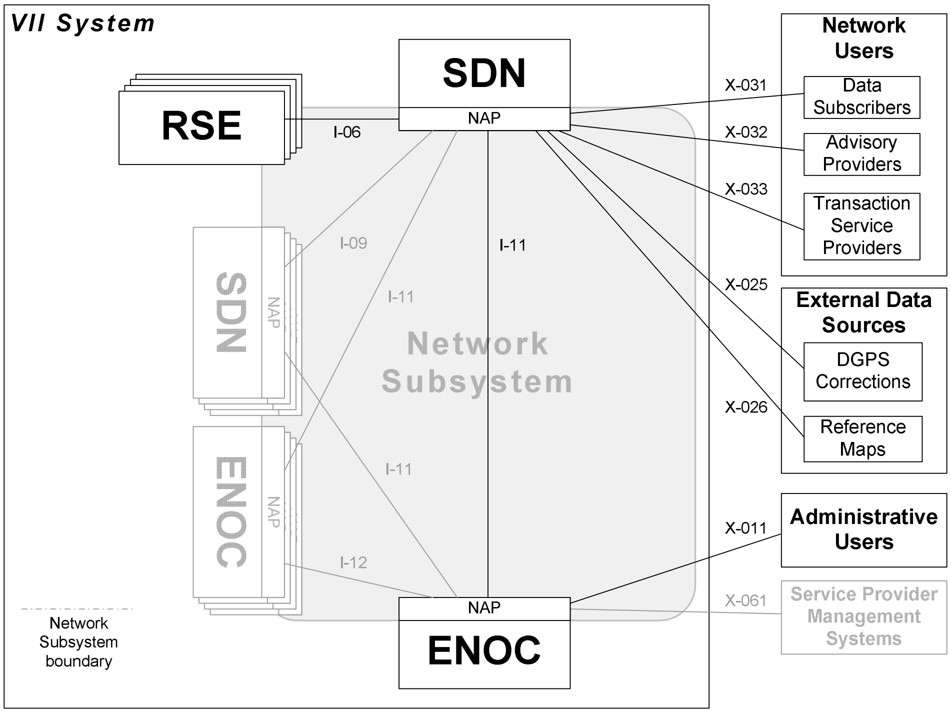
The Network Subsystem uses a standard terminology in defining the specific requirements. Definitions for these terms appear in *VII Infrastructure Lexicon*, which is a separate document (Reference 4).

2 NETWORK SUBSYSTEM DESCRIPTION

2.1 SUBSYSTEM PERSPECTIVE

Efficient and consistent delivery of VII services requires a robust, reliable infrastructure that interconnects the various components of the VII System. Vehicles must communicate with the roadside to reach services and applications; network users must be able to access data collected by the services; and the entire system must be managed and operated by the VII Operating Entity. The Network Subsystem is the communications infrastructure which enables data to be transported between Roadside Equipment and users of the VII System. The Network Subsystem is expected to be a geographically distributed collection of interconnected nodes that provide localized network services, managed by a centralized ENOC, as seen in Figure 2-1. Each of these nodes includes a Network Access Point (NAP), which is a communications hub that facilitates and controls connectivity between VII System components as well as providing controlled access for Network Users. The SDN and ENOC nodes also contain various servers that host applications and services for the VII System. The SDN servers host applications and services used by Network Users and External Data Sources (X-031, X-032, X-033, X-025, and X-026 in Figure 2-1), and the ENOC servers host applications and services used by Administrative Users (X-011 in Figure 2-1). The term Infrastructure Servers is used to reference both of these two distinct sets of servers together.

Figure 2-1: Network Subsystem



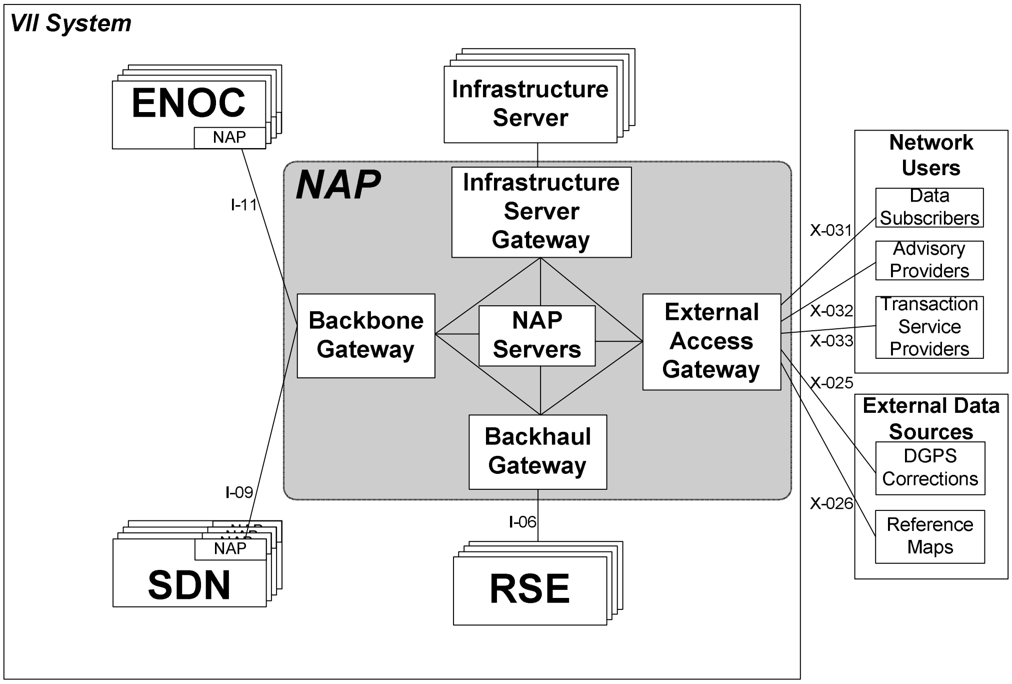
Specifically, the Network Subsystem will transport Internet Protocol (IP) traffic between—

- Instances of the SDN Subsystem [I-09]
- The SDN Subsystem and the ENOC Subsystem [I-11]
- Instances of the ENOC Subsystem [I-12]
- The SDN Subsystem and the RSE Subsystem [I-06]

Additionally, the Network Subsystem will enable Network Users, External Data Sources, and Administrative Users to communicate with the RSEs, the vehicles connected to the RSEs, and to the Infrastructure Servers located within the SDN and ENOC instances.

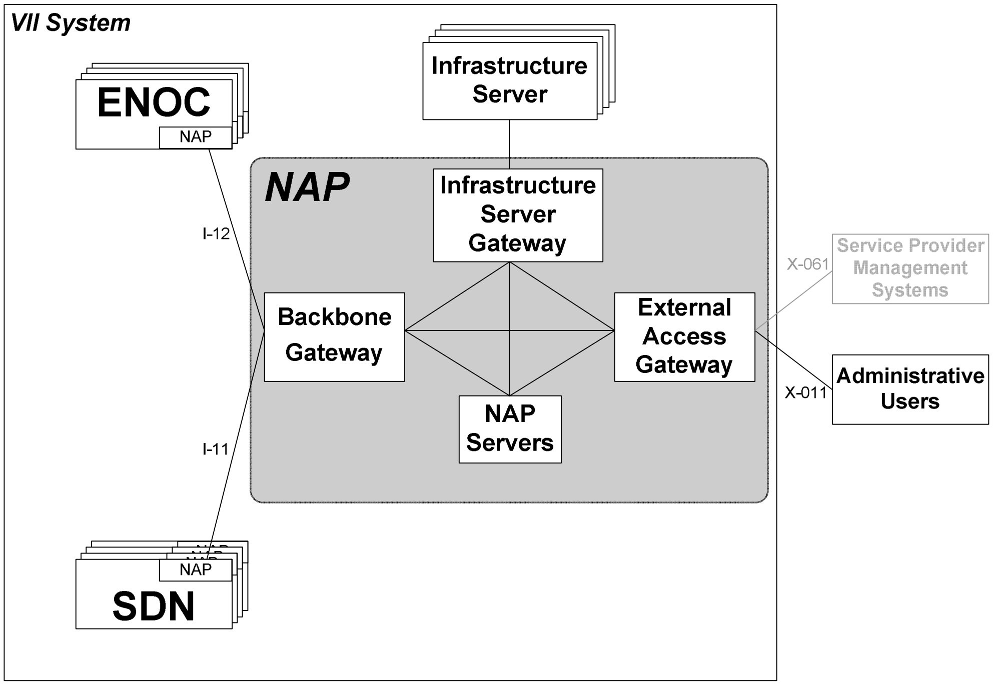
The primary nodes in the architecture are the Service Delivery Nodes (SDNs). These nodes will provide the primary network connectivity to the installed RSE Subsystems. Each SDN Subsystem Instance will include a NAP. This NAP will be composed of multiple gateways consisting of routers, firewalls, and intrusion detection systems (see Figure 2-2). Each of these gateways will be dedicated to support the respective connectivity to multiple nearby RSE Subsystems, multiple nearby Network Users, or two or more other SDN Subsystem Instances using the SDN to SDN [I-09] interface as shown in Figure 2-2. For a full description of the VII System Architecture, see the *VII National System Requirements* (Reference 1).

Figure 2-2: SDN NAP Functional Diagram



There will also be a NAP located in the ENOC, which is depicted in Figure 2-3. The primary difference between the SDN NAP in Figure 2-2 and the ENOC NAP in Figure 2-3 is the omission of the RSE Backhaul Gateway, which is not a necessary function of the ENOC.

Figure 2-3: ENOC NAP Functional Diagram

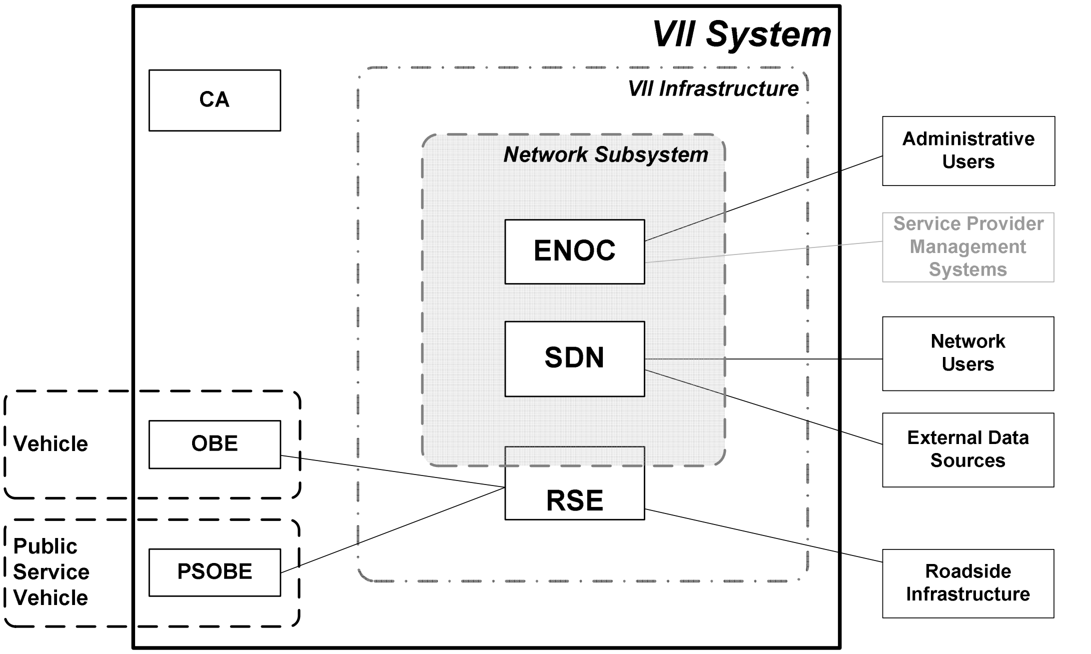


The Network Subsystem will support a number of VII System Services by providing connectivity between External System Users (e.g., Network Users) and the RSE Subsystem. In addition, with a co-located NAP, the SDN Subsystem supports communications between External System Users and the OBE Subsystem The remainder of this document defines requirements that specify how the Network Subsystem interconnects the other components of the VII infrastructure and provides basic communications services.

2.2 VII INFRASTRUCTURE

The term VII Infrastructure refers to a logical grouping of subsystems which fall under the responsibility of the VII Operating Entity. This grouping will contain the SDN Subsystem, the ENOC Subsystem, the RSE Subsystem and the Network Subsystem. The Operating Entity will not be responsible for the OBE Subsystem. Therefore, while the OBE Subsystem will be a part of the VII System, it will not be considered a part of VII Infrastructure. The relationship between the Network Subsystem and VII Infrastructure is illustrated in Figure 2-4.

Figure 2-4: The Network Subsystem inside VII Infrastructure



Note:
The External Data Source **GPS Signals**, which connects to several VII Subsystems, is not shown for clarity.

2.3 CONNECTIVITY

One of the primary functions of the Network Subsystem is to provide physical and logical connectivity between the geographically dispersed nodes and devices. As shown in Figure 2-1, the Network Subsystem will consist of interconnected NAPs. It is envisioned that each SDN Subsystem instance and ENOC Subsystem instance will contain a NAP. Each NAP will consist of multiple gateways composed of Network Devices and Security Devices, Each gateway within a NAP will handle a specific set of endpoint-to-endpoint transport interfaces, and be connected with either WAN or LAN links as appropriate. The transport interfaces have been defined as one of four types:

- **Backbone.** Provides connectivity between instances of the SDN Subsystem and between the SDN Subsystem and the ENOC Subsystem. The Backbone will also connect instances of the ENOC Subsystem with each other.
- **External Access.** Provides connectivity between external users, such as Data Subscribers, Advisory Providers, Transaction Service Providers, Differential Global Positioning Service (DGPS) Correction sources, and Reference Map sources and a given SDN.
- **RSE Backhaul.** Provides connectivity between a SDN and RSE devices.

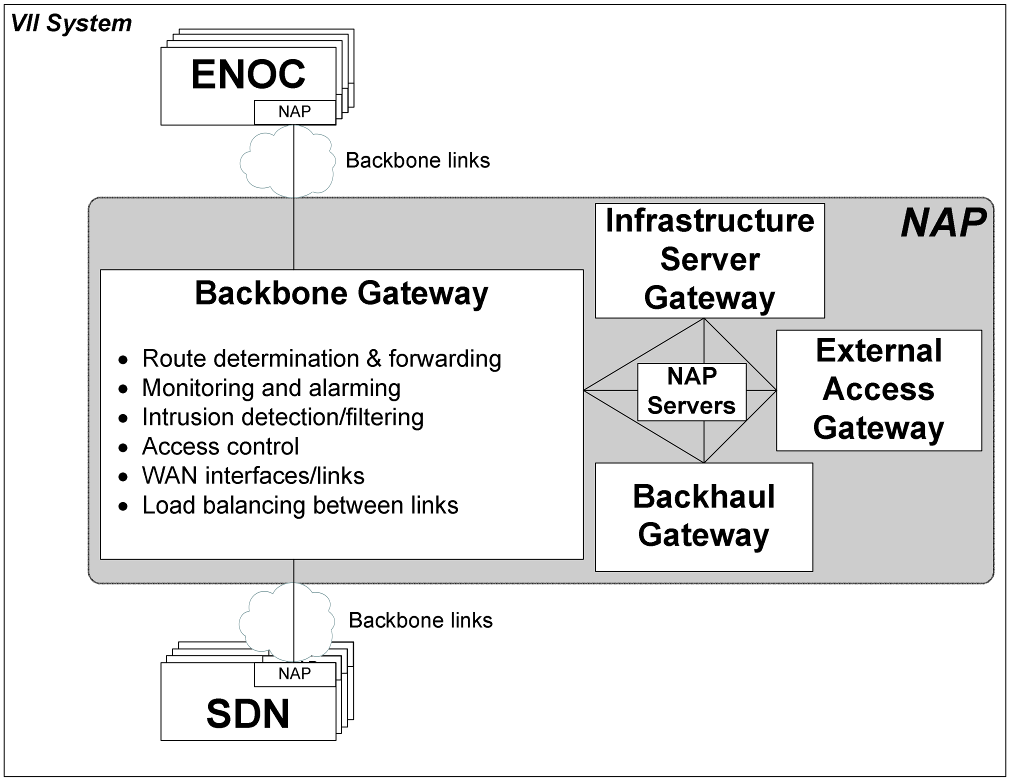
- **Infrastructure Server Transport.** Provide connectivity between the NAPs and associated Infrastructure Servers inside SDN Subsystem instances and ENOC Subsystem instances.

These Gateways and transport interfaces are discussed in detail below.

2.3.1 Backbone

The Backbone provides connectivity between geographically dispersed instances of the SDN and ENOC Subsystems. Each Backbone Gateway will be made up of interconnected Network Devices and Security Devices operating as a part of the NAP within a SDN or ENOC Subsystem instance. A Backbone Transport Interface refers to two specific Backbone Gateways and the communications link between them. As shown in Figure 2-5, each SDN or ENOC Subsystem instance will be logically homed to a minimum of two other Subsystem instances through physically diverse routes.

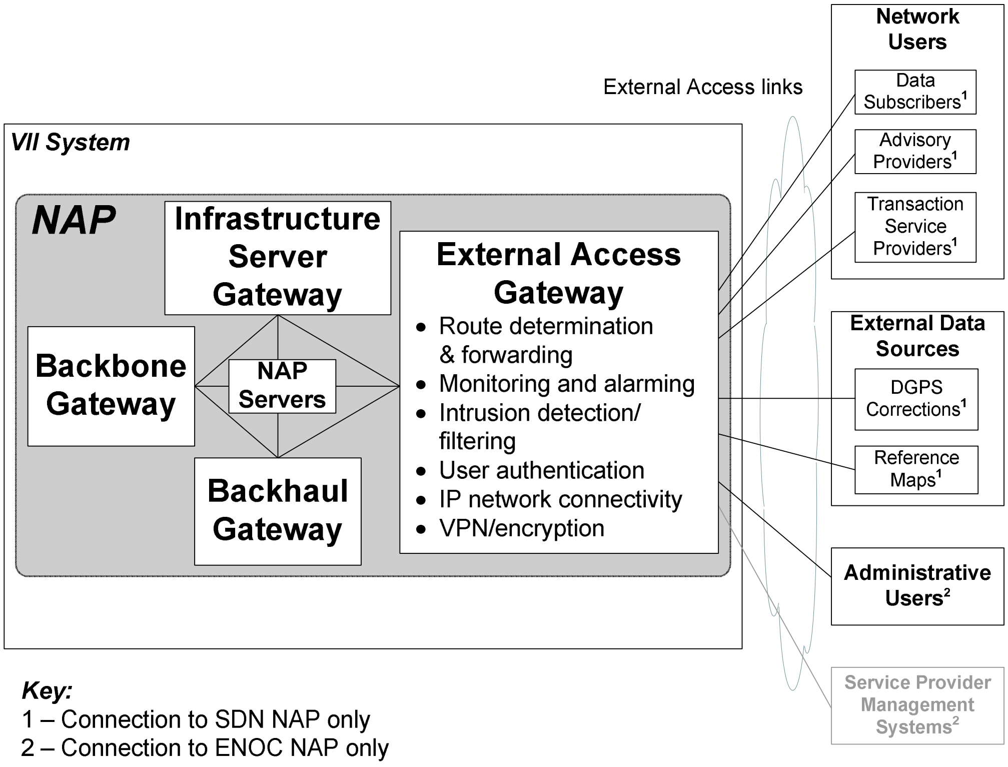
Figure 2-5: Backbone Gateway



2.3.2 External Access

An External Access Gateway is a combination of Network Devices and Security Devices that provides connectivity to parties external to the VII Network Subsystem. Figure 2-6 illustrates the role an External Access Gateway performs. Traffic between the VII System and Network Users, Administrative Users, Service Provider Management Systems, and selected External Data Sources will pass through an External Access Gateway. External Access Gateways will be distributed throughout the United States, but each Administrative User, Data Subscriber, Advisory Provider, and Transaction Service instance will have an assigned single entry point into the VII System, meaning the External Access Gateway of a specific NAP.

Figure 2-6: External Access Gateway


External Access links
VII System
NAP
Infrastructure Server Gateway
Backbone Gateway
NAP Servers
Backhaul Gateway
External Access Gateway
• Route determination & forwarding
• Monitoring and alarming
• Intrusion detection/ filtering
• User authentication
• IP network connectivity
• VPN/encryption
Network Users
Data Subscribers1
Advisory Providers1
Transaction Service Providers1
External Data Sources
DGPS Corrections1
Reference Maps1
Administrative Users2
Service Provider Management Systems2
Key:
1 – Connection to SDN NAP only
2 – Connection to ENOC NAP only

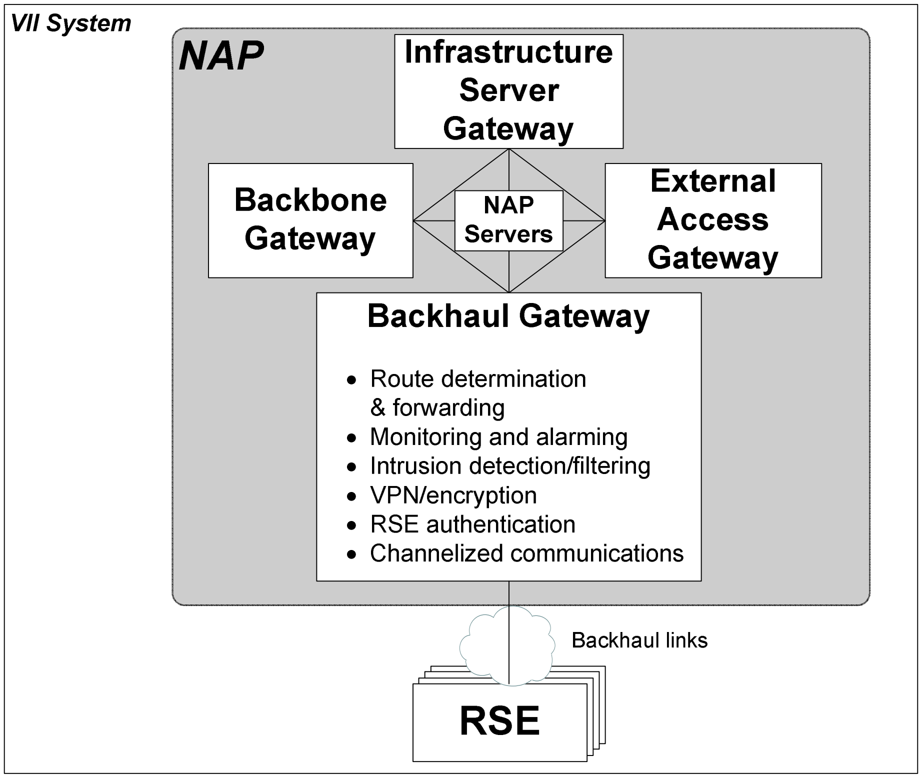
An External Access Transport Interface is defined as a connection between the VII System and an Administrative User, Network User, or selected External Data Source, consisting of a communications link and its two terminating endpoints. On the VII end of an External Access Transport Interface, the data traffic will typically enter and leave External Access Gateways through aggregated high-capacity communications links accommodating many Network Users. A dedicated communications link between an External Access Gateway and a specific Network User or External Data Source is also feasible. The specifics surrounding the engineering of the opposite end of each External Access Transport Interface, meaning at the facilities of Network Users or External Data Sources, is left to the Network User or External Data Source.

For the Proof of Concept, External Access will support transport of IP traffic between the VII System and both Network Users and Administrative Users, as well as Reference Maps and DGPS Corrections. For the national deployment, External Access will also provide access to the VII System for Service Provider Management Systems.

2.3.3 RSE Backhaul

RSE Backhaul will provide bi-directional transport of IP traffic between the SDN Subsystem and the RSE Subsystem in support of all services provided by the VII System. Backhaul traffic will enter and leave each SDN Subsystem instance through an RSE Backhaul Gateway. As shown in Figure 2-7, an RSE Backhaul Gateway will be a combination of Network Devices and Security Devices operating at the NAP within each SDN Subsystem instance. Technologies to be used in the RSE Backhaul may vary from location to location and depend on availability. For instance, in the national deployment these technologies may include but not be limited to T1/Fractional T1, T3, analog phone lines, Integrated Services Digital Network (ISDN), Frame Relay, cable modem, Digital Subscriber Line (DSL), 802.11-based wireless, dedicated microwave, free space optics, WiMAX, or digital cellular. It is anticipated that a subset of these technologies will be demonstrated in the Proof of Concept.

Figure 2-7: RSE Backhaul Gateway

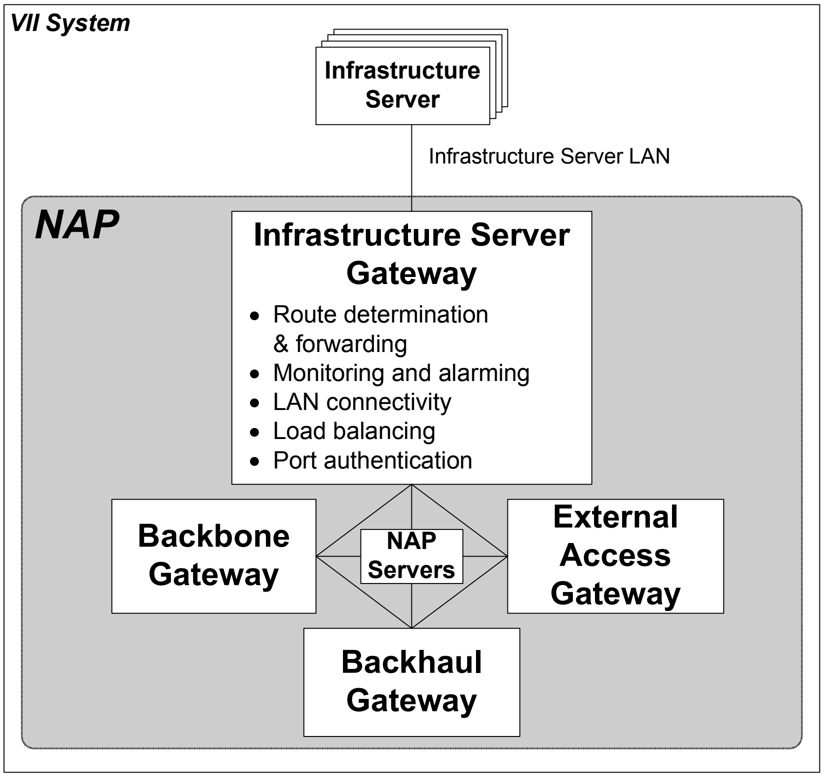

VII System
NAP
Infrastructure Server Gateway
Backbone Gateway
NAP Servers
External Access Gateway
Backhaul Gateway
• Route determination & forwarding
• Monitoring and alarming
• Intrusion detection/filtering
• VPN/encryption
• RSE authentication
• Channelized communications
Backhaul links
RSE

Each RSE Subsystem instance will be assigned to a specific primary SDN Subsystem instance. In the national deployment, each RSE Subsystem instance will have one link to its primary SDN Subsystem instance and a second (backup) link to its designated secondary SDN Subsystem instance. The backup link will be activated when either the primary SDN Subsystem instance fails or the communications link to the primary SDN Subsystem instance fails. This failover strategy requires that each SDN Subsystem instance maintains a certain amount of spare capacity. Further research and studies are required to determine the appropriate minimum, average, and maximum number of RSE Subsystem instances that should be served by a single SDN Subsystem instance.

2.3.4 Infrastructure Server Transport

Infrastructure Server Transport will provide bi-directional transport of IP traffic between the NAP and associated Infrastructure Servers. Whenever the NAP receives a data packet that needs to be processed by an Infrastructure Server in the same SDN Subsystem or ENOC Subsystem instance, the Server Transport will forward that packet to the appropriate Infrastructure Server. Conversely, whenever an Infrastructure Server sends out a packet to a destination outside the given SDN Subsystem instance or ENOC Subsystem instance, an Infrastructure Server Gateway will forward that packet to one (or more) of the three other Gateways. Infrastructure Server Gateways will use LANs and are envisaged as Layer 3 switches, using high-speed Ethernet connections, as illustrated in Figure 2-8.

Figure 2-8: Infrastructure Server Gateway



2.4 COMMUNICATIONS SERVICES

Communications Services refer to Network Subsystem services that provide data transport between Network Users and public and private vehicles. Communications Services include support for Classes of Service, Domain Name Service (DNS), address assignment, and a consistent time source throughout the network. They also include mobility management, i.e., management of application data traffic between Network Users and public and private vehicles as vehicles disconnect from one RSE Subsystem instance and reconnect at the same or another RSE Subsystem instance.

2.4.1 Classes of Service

To support some of the more critical services documented in the *VII National System Requirements*, the Network Subsystem must support different classes of service to enable the prioritization of network traffic. The Network Subsystem will use QoS mechanisms to support differential treatment of packets that flow thought the network and manage network resources during times of congestion. The Network Subsystem design document will define several distinct classes of service and performance guarantees for each class of service. During times of congestion, packets marked with a higher class of service, such as a flash flood or hurricane warning, may receive priority over a lower class of service, such as a vehicle service message from an auto manufacturer. Likewise, messages intended to clear the way for an ambulance may be transmitted before packets executing a commercial electronic transaction.

2.4.1.1 Traffic Classification

For the Network Subsystem to provide a differentiated treatment of packets in the VII network, the packets need to be classified and the headers appropriately marked so network devices and security devices can process the packets according to the specified class of service.

The Proof of Concept will support a minimum of two classes of service. For the Proof of Concept, it is expected that all packets entering the Network Subsystem will be classified and marked with a class of service based on the type of traffic. Unmarked packets entering the Network Subsystem will, by default, be marked with the lowest class of service.

2.4.1.2 Traffic Conditioning

Traffic entering and exiting the VII Network Subsystem may be subject to one or more traffic conditioning actions to support prioritization of specific classes of service. This is to ensure that the incoming traffic profile conforms to any rules specified in the network management policies. Traffic conditioning can involve delaying packets to bring the data stream in compliance with a traffic profile as well as marking of packet headers with values that translate into specific forwarding behaviors.

2.4.1.3 Traffic Forwarding

Each class of service will be allocated a guaranteed amount of bandwidth on the egress interface. In times of congestion, the network devices will drop packets exceeding the bandwidth allocated for each class of service. Unused bandwidth assigned to a class of service may be used to send traffic marked with other classes of service during periods of non-congestion. During times of congestion, traffic conditioning mechanisms will be used to prevent forwarded packets from exceeding the guaranteed bandwidth on the egress interface. The traffic forwarding behavior determines the priority and drop precedence of traffic about to be forwarded on the network. After a value is placed in the packet header, the packet forwarding behavior is determined by the forwarding scheme used by QoS marking-aware nodes in the network.

2.4.2 Domain Name Service (DNS)

Domain Name Service (DNS) is a critical service within the VII System. Due to the number of devices and the size of IPv6 addresses, an efficient DNS is essential for the proper end-to-end operation of the VII environment. Not only will it be important that devices be given easy to remember names, but OBE and PSOBE will need to quickly determine how to access various services. Given that the physical addresses may vary from RSE to RSE, it is essential that names be clearly delimited.

The VII Network DNS will support both IPv4 and IPv6 in the Proof of Concept network. Requests from Managed Entities, including users and network devices, will be authorized and filtered to maintain any required separations (such as between network users). Administrative users and system operators will have the ability to create, read, update, and delete authorized DNS entries.

For the national rollout, the VII Network DNS will have two distinct zones – one internal and one external. The internal DNS will include all managed devices in the network and enable the ENOC users to access all devices as required. The external DNS will be a subset of the internal DNS, containing only those records necessary for external users. This will prohibit external users from accessing unauthorized nodes and devices. Each External Access gateway will have an associated DNS server that will provide DNS services for external users that connect using that gateway. Each SDN will also have an associated DNS server for use by the devices within the SDN, including servers, routers, RSEs, and security appliances. One ENOC will contain the two master servers for the entire VII network – one for the internal DNS servers, and one for the external DNS servers. The master external DNS server will be a slave to the master internal DNS server, which is where the records for transmission to the external DNS servers will be stored. All other DNS servers in the network will get their information from these master servers. As necessary, secondary and tertiary levels of servers will be defined to distribute the traffic throughout the network. For each master DNS server, another server within the network will be designated as the secondary DNS for that location. In the event that the primary server fails, the secondary will take over the responsibilities for that SDN.

Additionally in the national rollout, the DNS capabilities will be extended to include support for unique address resolutions for a single logical name based on the RSE from which the request originates. This will allow the VII network operations and network users to define – on an RSE basis – the servers that will support any given service. As an example, one RSE may be using a local server while another RSE uses a server in a different part of the country. This would happen transparently to the OBE or PSOBE using the provided service. Thus, special situations and load balancing requirements can be addressed.

2.5 PROTOCOLS

Several protocols will be necessary in order to deliver VII Services. In the national deployment, the Network Subsystem will rely on Internet Protocol version 6 (IPv6) to route data packets between their sources and destinations. For the Proof of Concept, the Network Subsystem will use both IPv6 and Internet Protocol version 4 (IPv4). In addition, several other standard Internet protocols will be supported:

- DNS
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- Network Time Protocol (NTP).

The Network Subsystem will also use the suite of protocols associated with IPv6 to support routing, message prioritization, network management, and security functions. Protocols required for the Network Subsystem are specified in Section 4.3. Additional information about these protocols and the communications services they support will be in a future version of this document.

2.6 CLASSES OF SERVICE

The Network Subsystem will use message differentiation mechanisms to allow certain messages to be delivered ahead of others or to provide special treatment to certain types of messages. These differentiation mechanisms will define several distinct classes of service. For example, a flash flood warning or a hurricane warning may receive priority over a vehicle service message from an auto manufacturer. Likewise, messages intended to clear the way for an ambulance may be transmitted before packets executing a commercial electronic transaction. The Proof of Concept will support a minimum of two classes of service.

2.7 NETWORK MANAGEMENT

The Network Subsystem will be capable of using SNMP versions 1, 2c, and 3. The NAP within the SDN Subsystem consists of Network Devices and Security Devices and these will use Version II of Management Information Base for Network Management of TCP/IP-based Internets (MIB II).

The ENOC Subsystem will fulfill network management functions with respect to the SDN Subsystem (including the NAP) and the RSE Subsystem. The ENOC Subsystem provides a centralized monitoring and control function for the VII Network and all (non-mobile) VII System components. The ENOC Subsystem will also provide for analysis and report generation in support of long-term trending and planning activities. In the national deployment of VII, network management tools will be used for remote provisioning, configuration, and monitoring of RSE Subsystem instances throughout the VII System.

For additional information on this interface see the *VII Enterprise Network Operations Center (ENOC) Subsystem to Service Delivery Node (SDN) Subsystem [I-11] Software Interface Requirements Specification* (Reference 17).

2.8 SECURITY

The Network Subsystem will employ a range of controls to protect the network from unauthorized access and preserve the confidentiality and integrity of transmitted data. Specific security requirements are presented in the Security subsection of the Network Subsystem Specification. These requirements call for the use of security and cryptographic standards, protocols, and functions to secure the Network Subsystem. The Network Subsystem shall employ a number of security controls to provide confidentiality, integrity, and availability for the network itself, as well as for services provided by other subsystems. Examples of security controls to be used include network-level encryption technologies, firewall/filtering technologies, auditing/intrusion detection technologies, and Identity and Access Management (IdAM) services. Security controls for the POC will support both IPv6 and IPv4.

2.9 PERFORMANCE

Performance for the Network Subsystem is generally defined in terms of scalability, availability, and reliability. Scalability means the ability to significantly increase capacity of the subsystem over a period of time without having to replace the equipment that was used in the initial deployment of the subsystem. Although scalability requirements for the national deployment are yet to be determined, the Proof of Concept by design has no scalability requirement given that it is intended to demonstrate the functional requirements of the system and cannot adequately demonstrate scalability because of its inherent limitations. To arrive at meaningful scalability requirements, further analysis will need to be conducted to estimate the expected traffic volumes and processing loads at the time of initial national deployment and to project the growth of the VII System over time.

Availability and reliability refer to the Network Subsystem's ability to perform its functions continuously. Availability is tied to such concepts as failover, redundancy, and hot standby. The Proof of Concept is focused on proving functional capabilities, with less focus on availability and reliability—the Network Subsystem is not required to eliminate single points of failure. Availability and reliability requirements will be developed after a detailed analysis. They will be included in a future document for the national deployment.

Additional performance requirements will be included in a future version of this document.

3 GENERAL NETWORK REQUIREMENTS

No general network requirements have been identified in this document.

4 FUNCTIONAL REQUIREMENTS

4.1 CONNECTIVITY

4.1.1 End-to-End

REQ #	REQUIREMENT	POC	NATIONAL
NTWK8	The Network Subsystem shall provide connectivity between the Gateways within a Network Access Point.	Yes	Yes
NTWK41	The Network Subsystem shall provide local area network connectivity between all Managed Network Elements and servers within a given physical location.	Yes	Yes
NTWK48	The Network Subsystem shall not be disabled by the failure of any single element of the Network Subsystem.	No	Yes
NTWK50	The Network Subsystem shall support non-proprietary physical connectors only.	Yes	Yes
NTWK250	The Network Subsystem shall use outdoor-rated cabling for all outside plant cabling.	Yes	Yes

4.1.2 Backbone

REQ #	REQUIREMENT	POC	NATIONAL
NTWK83	The Network Subsystem shall support logical homing of each SDN Subsystem instance to at least two (2) other SDN Subsystem instances.	No	Yes
NTWK311	The Network Subsystem shall provide at least two diversely routed Backbone Transport Interfaces for each facility housing SDN or ENOC Subsystem equipment.	No	Yes
NTWK352	The Network Subsystem shall provide connectivity between two instances of the SDN Subsystem through a Backbone Transport Interface.	Yes	Yes
NTWK353	The Network Subsystem shall provide connectivity between an SDN Subsystem instance and an ENOC Subsystem instance through a Backbone Transport Interface.	Yes	Yes
NTWK354	The Network Subsystem shall allow connectivity between two instances of the ENOC Subsystem through a Backbone Transport Interface.	No	Yes

4.1.3 External Access

REQ #	REQUIREMENT	POC	NATIONAL
NTWK51	The Network Subsystem shall support communications between Network Users and the SDN Subsystem.	Yes	Yes
NTWK345	The Network Subsystem shall provide connectivity between a Network User and the VII System through an External Access Transport Interface.	Yes	Yes
NTWK346	The Network Subsystem shall provide connectivity between an Administrative User and the VII System through an External Access Transport Interface.	Yes	Yes
NTWK347	The Network Subsystem shall provide connectivity between a Service Provider Management System and the VII System through an External Access Transport Interface.	No	Yes
NTWK349	The Network Subsystem shall provide connectivity between a network-based DGPS corrections source and the VII System through an	Yes	Yes

REQ #	REQUIREMENT	POC	NATIONAL
	External Access Transport Interface.		
NTWK350	The Network Subsystem shall provide connectivity between a source of Reference Maps and the VII System through an External Access Transport Interface.	Yes	Yes

4.1.4 RSE Backhaul

REQ #	REQUIREMENT	POC	NATIONAL
NTWK31	The Network Subsystem shall be configured to support any combination of defined RSE Backhaul Transport Interface types between each instance of the SDN Subsystem and its assigned RSE Subsystem instances.	Yes	Yes
NTWK34	The Network Subsystem shall allow connection with up to 100 RSE Subsystem instances to each SDN Subsystem instance.	Yes	No
NTWK61	The Network Subsystem shall support communications between each instance of the SDN Subsystem and its assigned instances of the RSE Subsystem.	Yes	Yes
NTWK249	The RSE Backhaul Transport Interface shall be configurable to support connectivity between an RSE Subsystem instance and its primary SDN Subsystem instance and its secondary SDN Subsystem instance.	No	Yes
NTWK351	The Network Subsystem shall provide connectivity between a SDN Subsystem instance and a RSE Subsystem instance through a RSE Backhaul Transport Interface.	Yes	Yes

4.1.5 Infrastructure Server Transport

REQ #	REQUIREMENT	POC	NATIONAL
NTWK356	The Network Subsystem shall provide connectivity between SDN Servers and a Network Access Point collocated within the same instance of the SDN Subsystem through Server Transport Interfaces.	Yes	Yes
NTWK357	The Network Subsystem shall provide connectivity between ENOC Servers and a Network Access Point collocated within the same instance of the ENOC Subsystem through Server Transport Interfaces.	Yes	Yes

4.2 Communications Services

4.2.1 Classes of Service

REQ #	REQUIREMENT	POC	NATIONAL
NTWK75	The Network Subsystem shall support at least two Classes of Service.	Yes	No
NTWK360	The Network Subsystem shall support at least four Classes of Service.	No	Yes
NTWK361	The Network Subsystem shall provide a guaranteed minimum bandwidth for each Class of Service.	Yes	Yes
NTWK362	The Network Subsystem shall support packet prioritization.	Yes	Yes
NTWK363	The Network Subsystem shall support different packet priority levels based on Classes of Service.	Yes	Yes
NTWK364	The Network Subsystem shall have the ability to classify and mark packets with a Class of Service.	No	Yes
NTWK365	The Network Subsystem shall associate each VII service with a specific Class of Service based on network management policies.	No	Yes

REQ #	REQUIREMENT	POC	NATIONAL
NTWK366	The Network Subsystem shall accept and forward packets marked by Administrative Users, Network Users, and External Data Sources.	Yes	Yes
NTWK367	The Network Subsystem shall ensure that any unmarked packets will be given the lowest supported Class of Service.	Yes	Yes
NTWK368	The Network Subsystem shall ensure that marked packets originating from System Users are appropriately marked according to the active policy.	No	Yes
NTWK369	The Network Subsystem shall support the ability to perform Traffic Conditioning.	Yes	Yes
NTWK452	The Network Subsystem shall accept and forward marked packets from the RSE Subsystem.	Yes	Yes

4.2.2 Domain Name Service (DNS)

REQ #	REQUIREMENT	POC	NATIONAL
NTWK370	The Network Subsystem shall support the Domain Name Service to provide logical names for Managed Network Elements.	Yes	Yes
NTWK371	The Network Subsystem shall support the Domain Name Service to provide logical names associated with network addresses of Transaction Service Providers.	Yes	Yes
NTWK372	The Network Subsystem shall maintain a master repository for Managed Network Element logical names.	Yes	Yes
NTWK373	The Network Subsystem shall support distributed repositories replicated from the master logical name repositories.	No	Yes
NTWK374	The Network Subsystem shall support Domain Name Service queries and responses over IPv4.	Yes	No
NTWK375	The Network Subsystem shall provide the Domain Name Service for IPv4 addresses.	Yes	No
NTWK376	The Network Subsystem shall support partitioned Domain Name Service services for devices and users internal to the VII Infrastructure and for devices and users external to the VII Infrastructure.	No	Yes
NTWK377	The Network Subsystem shall authorize and filter Domain Name Service queries from Managed Entities.	No	Yes
NTWK378	The Network Subsystem shall support multiple IP addresses per Domain Name Service logical name.	No	Yes
NTWK379	The Network Subsystem shall have the ability to provide the response to a Domain Name Service query originating from a Vehicle or Public Service Vehicle based on the associated RSE Subsystem instance.	No	Yes
NTWK380	The Network Subsystem shall provide a means for authorized Administrative Users and System Operators to Create, Read, Update and Delete (CRUD) authorized Domain Name Service entries.	No	Yes
NTWK383	The Network Subsystem shall maintain a Domain Name Service entry for each Managed Network Element in the VII Infrastructure.	Yes	Yes
NTWK427	The Network Subsystem shall maintain a master repository for Transaction Service Provider logical names.	Yes	Yes
NTWK428	The Network Subsystem shall support Domain Name Service queries and responses over IPv6.	Yes	Yes
NTWK429	The Network Subsystem shall provide the Domain Name Service for IPv6 addresses.	Yes	Yes

4.2.3 Time Service

REQ #	REQUIREMENT	POC	NATIONAL
NTWK332	The Network Subsystem shall use Coordinated Universal Time (UTC).	Yes	Yes
NTWK333	The Network Subsystem shall synchronize all time clocks with, at a minimum, a Stratum-2 time source.	Yes	Yes

4.3 Protocols

REQ #	REQUIREMENT	POC	NATIONAL
NTWK1	The Network Subsystem shall have the ability to deliver Internet Protocol (IP) packets from a single source to a single destination.	Yes	Yes
NTWK2	The Network Subsystem shall have the ability to deliver Internet Protocol (IP) packets from a single source to multiple destinations.	Yes	Yes
NTWK14	The Network Subsystem shall support the transport of Internet Protocol version 4 (IPv4) packets.	Yes	No
NTWK15	The Network Subsystem shall support the transport of Internet Protocol version 6 (IPv6) packets.	Yes	Yes
NTWK16	The Network Subsystem shall support Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) simultaneously.	Yes	No
NTWK17	The Network Subsystem shall support multicast under Internet Protocol version 6 (IPv6).	No	Yes
NTWK18	The Network Subsystem shall support the Internet Group Management Protocol version 3 (IGMPv3).	No	Yes
NTWK20	The Network Subsystem shall support the Multicast Listener Discovery (MLD) protocol.	No	Yes
NTWK23	The Network Subsystem shall support RIP version 2, OSPF version 2 and BGP version 4 protocols.	Yes	No
NTWK24	The Network Subsystem shall support RIPng, OSPF version 3, and BGP version 4 protocols.	Yes	Yes
NTWK27	The Network Subsystem shall support the Address Resolution Protocol (ARP).	Yes	No
NTWK28	The Network Subsystem shall support the Internet Control Message Protocol version 6 (ICMPv6).	Yes	Yes
NTWK115	The Network Subsystem shall support appropriate protocol(s) so as to ensure failover to a stand-by network or security device in case of failure of any Network Device or Security Device.	No	Yes
NTWK278	The Network Subsystem shall support the Internet Control Message Protocol version 4 (ICMPv4).	Yes	No
NTWK279	The Network Subsystem shall support the Neighbor Discovery (ND) protocol.	Yes	Yes
NTWK358	The Network Subsystem shall support Integrated IS-IS protocol.	No	Yes

4.4 Network Management

REQ #	REQUIREMENT	POC	NATIONAL
NTWK21	The Network Subsystem Managed Network Elements shall support the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3.	Yes	Yes
NTWK334	The Network Subsystem shall only allow management access from the	Yes	Yes

REQ #	REQUIREMENT	POC	NATIONAL
	ENOC Subsystem.		
NTWK335	The Network Subsystem shall generate network/element fault management data.	Yes	Yes
NTWK336	The Network Subsystem shall forward all network/element management data to the ENOC Subsystem.	Yes	Yes
NTWK337	The Network Subsystem shall execute management commands from the ENOC Subsystem.	Yes	Yes
NTWK338	The Network Subsystem shall generate network/element performance management data.	Yes	Yes
NTWK339	The Network Subsystem shall generate network/element configuration management data.	Yes	Yes
NTWK340	The Network Subsystem shall generate network/element accounting management data.	No	Yes
NTWK341	The Network Subsystem shall generate SNMP MIB-II (trap) Alarms.	Yes	Yes
NTWK342	The Network Subsystem shall generate SNMP MIB-III (trap) Alarms.	No	Yes
NTWK343	The Network Subsystem shall have the ability to generate a "keepalive" Message.	Yes	Yes
NTWK344	The Network Subsystem shall have the ability to configure the time interval of "keepalive" messages.	Yes	Yes

4.5 SECURITY

REQ #	REQUIREMENT	POC	NATIONAL
NTWK280	The Network Subsystem shall use MD-5 hashing to authenticate routing updates when using the RIPng protocol.	Yes	Yes
NTWK281	The Network Subsystem shall use IPSec Authentication Header to authenticate routing updates when using the OSPFv3 protocol.	Yes	Yes
NTWK282	The Network Subsystem shall use MD-5 hashing to authenticate routing updates when using the Integrated IS-IS protocol.	No	Yes
NTWK283	The Network Subsystem shall use IPSec Authentication Header or Encapsulated Security Payload protocols to authenticate routing updates when using the BGP protocol.	Yes	Yes
NTWK284	The Network Subsystem shall have the ability to filter traffic between VII services.	Yes	Yes
NTWK285	The Network Subsystem shall support the use of Internet Key Exchange (IKE) version two (2) per RFC 4306.	No	Yes
NTWK286	The Network Subsystem shall support the use of cryptographic algorithms for IPSec per RFC 4305.	Yes	Yes
NTWK287	The Network Subsystem shall support the use of IEEE 802.1x, for port authentication.	Yes	Yes
NTWK288	The Network Subsystem shall statically configure the allowed MAC addresses (MAC Address Table) per port interface.	Yes	Yes
NTWK289	The Network Subsystem shall disable trunking on all access ports.	Yes	Yes
NTWK290	The Network Subsystem shall assign and configure only trunk ports to associated trunk VLANs.	Yes	Yes
NTWK292	The Network Subsystem shall disable all unused ports and place them in a dedicated non-operational VLAN.	Yes	Yes
NTWK294	The Network Subsystem shall authenticate access to the Subsystem's Managed Network Elements.	Yes	Yes

REQ #	REQUIREMENT	POC	NATIONAL
NTWK298	The Network Subsystem shall have the ability to detect security events.	Yes	Yes
NTWK299	The Network Subsystem shall have the ability to log security events.	Yes	Yes
NTWK300	The Network Subsystem shall forward security event log data to the ENOC Subsystem.	Yes	Yes
NTWK301	The Network Subsystem shall be able to collect session data.	Yes	Yes
NTWK302	The Network Subsystem shall be able to collect traffic flow records.	Yes	Yes
NTWK308	The Network Subsystem shall support the use of IKE version one (1) per RFC 4109.	Yes	No
NTWK309	The Network Subsystem shall use MD-5 hashing to authenticate routing when using the OSPFv2 protocol.	Yes	Yes
NTWK312	The Network Subsystem shall forward collected session data to the ENOC Subsystem.	Yes	Yes
NTWK313	The Network Subsystem shall be able to forward collected traffic flow records to the ENOC Subsystem.	Yes	Yes
NTWK328	The Network Subsystem's shall authenticate access to physical (console) ports.	No	Yes

5 PERFORMANCE REQUIREMENTS

There are no performance requirements in this version of the document. Detailed performance requirements will be specified in a future version of this document.

6 FACILITIES REQUIREMENTS

6.1 GENERAL

REQ #	REQUIREMENT	POC	NATIONAL
NTWK314	The facility housing Network Subsystem equipment shall have an air conditioning system capable of providing an ambient temperature of 72F (22C).	Yes	Yes
NTWK315	The facility housing Network Subsystem equipment shall not vary temperatures more than 10F (5.5C) per hour of operation.	Yes	Yes
NTWK316	The facility housing Network Subsystem equipment shall have an air conditioning system capable of providing a relative humidity of 45-50%.	Yes	Yes
NTWK317	The facility housing Network Subsystem equipment shall not vary the relative humidity more than 10% per hour of operation.	Yes	Yes
NTWK318	The facility housing Network Subsystem equipment shall have heat and smoke detectors that meet or exceed all local fire code regulations.	Yes	Yes
NTWK319	The facility housing Network Subsystem equipment shall have a special hazards fire protection system providing rapid fire detection, integrated emergency response, and waterless fire suppression.	Yes	Yes
NTWK320	The facility housing Network Subsystem equipment shall have separate grounding systems to prevent grounding loops.	Yes	Yes
NTWK321	The facility housing Network Subsystem equipment shall have a continuous power supply with a backup uninterruptible power supply(UPS).	Yes	Yes
NTWK323	The facility housing Network Subsystem equipment shall allow for the network equipment racks to be electrically grounded and secured(bolted) to the flooring.	Yes	Yes
NTWK324	The facility housing Network Subsystem equipment shall have two independent power outlets with independent circuit breakers, for each network equipment rack.	Yes	Yes

6.2 SECURITY

REQ #	REQUIREMENT	POC	NATIONAL
NTWK303	The Network Subsystem physical ports shall be secured in a locked compartment to prevent unauthorized access.	No	Yes
NTWK304	The Network Subsystem facilities shall be protected by physical access controls.	No	Yes
NTWK305	The Network Subsystem facility shall log physical access attempts.	No	Yes
NTWK327	The Network Subsystem facility shall forward all physical access logs to the ENOC Subsystem.	No	Yes

APPENDIX A: ASSUMPTIONS AND DEPENDENCIES

ASSUMPTIONS

ASSUMPTION ID	ASSUMPTION TEXT
ASU3	The Proof of Concept will have no more than 100 concurrently connected RSE Subsystems for each SDN Subsystem
ASU4	The Proof of Concept will have no more than three (3) concurrently connected SDN Subsystem instances
ASU5	An RSE Subsystem will collect and aggregate no more than 375 Probe Data Messages per second. This assumes (5 vehicles / lane / sec) * (10 lanes) * (30 Probe Data Snapshots / vehicle) / (4 Probe Data Snapshots / Probe Data Message)
ASU6	The Proof of Concept will have no more than one (1) ENOC Subsystem.
ASU9	The ENOC Subsystem will consist of the Management Service and the Security Service
ASU10	The ENOC subsystem shall use network management protocols which comply with recognized internetworking management standards
ASU11	The ENOC subsystem shall use recognized internetworking management standards for fault, configuration, accounting and performance management
ASU12	The ENOC subsystem shall use non standard network management protocols if necessary to manage specific managed network elements
ASU13	The ENOC subsystem shall be a platform comprised of multiple sub-components which together complete the requirements of the ENOC subsystem
ASU14	The ENOC subsystem shall capture and process configuring orders for all types of service and managed network elements
ASU15	ENOC operators will be able to access standard process documentation for handling reported incidents and requests for service.
ASU16	ENOC operators will be trained to follow standard process for handling reported incidents and requests for service.
ASU17	Roadside Equipment (RSEs) will support two types of digital certificates: IEEE 1609.2 for wireless communication and X.509v3 for network communication requirements.
ASU18	CA to SDN, CA to ENOC, RSE to SDN, and SDN to ENOC communication will use X.509 v3 compliant certificates for certificate-based activities.
ASU20	The VII wireless infrastructure (OBE, RSE) will use IEEE 1609.2 compliant certificates for certificate-based activities.
ASU21	Bridging of X.509 and IEEE 1609.2 Certificate Authorities will not be required.
ASU22	The VII CA Subsystem shall consist of two separate CA certificate systems: the X.509 CA, and the IEEE 1609.2 compliant CA.
ASU23	VII Infrastructure systems and devices will use X.509 certificates for digital signatures, encryption, and identification.
ASU25	All connections internal to the SDN and the NAP shall use Ethernet.

ASSUMPTION ID	ASSUMPTION TEXT
ASU26	A separate document will be created to specify requirements regarding electrical power supply, surge protection, physical space, humidity control, temperature control and similar environmental factors for the supporting facilities.
ASU27	The VII POC Environment shall have no more than 50 Network and/or Administrative Users.
ASU28	RSE Backhaul traffic flowing to and from RSE Backhaul Gateways will be aggregated by service providers.

DEPENDENCIES

DEPENDENCY ID	DEPENDENCY
DEP1	Probe Data Service (PDS) performance requirements are dependent upon the structure and size of the SAE J2735 Probe Data Message.
DEP2	Advisory Message Distribution Service (AMDS) performance requirements are dependent upon network transport availability.
DEP3	The implementation of ENOC management services is dependent on the establishment of network connectivity between the ENOC and the managed network elements.
DEP4	The implementation of ENOC security services is dependent on the establishment of network connectivity between the ENOC and the managed security elements
DEP5	A Network management agent is running in the managed network element and network connectivity exists between the managed network element and the ENOC
DEP6	The ENOC has connectivity to the managed network elements
DEP7	Connectivity with the ENOC Subsystem.
DEP8	The existence of a VII CA certificate repository.
DEP9	Hardware Security Modules (HSMs) capable of supporting required certificate assurance levels.
DEP10	A VII CA Certificate Practice Statement (CPS) describing the practices and standards to which the CA shall be managed.
DEP11	The VII System will support Lightweight Directory Access Protocol (LDAP) Version 3.0.
DEP12	The VII System will support Secure Lightweight Directory Access Protocol (LDAPS).
DEP13	The VII System will support Hypertext Transfer Protocol (HTTP).
DEP14	The VII System will support Secure Hypertext Transfer Protocol (HTTPS).

APPENDIX B: REFERENCE DOCUMENTS

REF #	REFERENCE	VERSION
1	VII National System Requirements	Version 1.2.1
2	VII Concept of Operations	Draft 1.2
3	VII Data Element Dictionary	Version 1.0
4	VII Infrastructure Lexicon	Version 1.1
5	VII System Infrastructure Security Plan	Version 2.1
6	VII USDOT Day-1 Use Case Descriptions (May 2006)	Version 1.0
7	VII x.509 Certificate Authority Certificate Practice Statement (CPS)	TBD
Subsystem Specification (SSS) Documents		
8	VII Certificate Authority (CA) Subsystem Specification (SSS)	Version 1.1
9	VII Enterprise Network Operations Center (ENOC) Subsystem Specification (SSS)	Version 1.1 -- Final
10	VII Network Subsystem Specification (SSS)	Version 1.1
11	VII Roadside Equipment (RSE) Subsystem Specification (SSS)	Version 1.0
12	VII Service Delivery Node (SDN) Subsystem Specification (SSS)	Version 1.1
Software Interface Requirements Specification (Software IRS) Documents		
13	VII Enterprise Network Operations Center (ENOC) to Administrative User [X-011] Software Interface Requirements Specification	Version 1.1
14	VII Enterprise Network Operations Center (ENOC) to Certificate Authority (CA) Subsystem [I-13] Software Interface Requirements Specification	Version 1.1
15	VII Enterprise Network Operations Center (ENOC) to Managed Entity (ME) [Managed Entity] Software Interface Requirements Specification	Version 1.1
16	VII Enterprise Network Operations Center (ENOC) to Managed Network Element (MNE) [I-08 and I-11] Software Interface Requirements Specification	Version 1.1
17	VII Enterprise Network Operations Center (ENOC) Subsystem to Service Delivery Node (SDN) Subsystem [I-11] Software Interface Requirements Specification	Version 1.1
18	VII Network User to Service Delivery Node (SDN) Subsystem [X-031, X-032, X-033] Software Interface Requirements Specification	Version 1.1
19	VII Service Delivery Node (SDN) Subsystem to Roadside Equipment (RSE) Subsystem [I-06] Software Interface Requirements Specification	Version 1.1
20	VII Service Provider Management Systems to SDN Subsystem IRS [X-061] *(Not in scope for POC)*	*Not in Scope*
Mapping Documents		
21	Reference Maps – TBD	TBD
22	Navstar GPS Space Segment/Navigation User Interfaces, ICD GPS 200	Revision C
Internet Engineering Task Force (IETF) Requests for Comments (RFCs)		
23	Internet Engineering Task Force (IETF) Request for Comments (RFC) 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols	© 1999
24	Internet Engineering Task Force (IETF) RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	© 2004
Dedicated Short Range Communications (DSRC) Documents		
25	Draft SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary	Rev. 15
26	POC Additions & Exceptions to the POC Version of SAE J2735	APP190-02

APPENDIX C: NATIONAL SYSTEM REQUIREMENTS TRACEABILITY

SUBSYSTEM SPECIFICATION ID	NSR SPECIFICATION ID
NTWK1	VF-COMM-01
	VF-COMM-02
	VF-COMM-03
NTWK2	VF-COMM-01
	VF-COMM-02
	VF-COMM-03
NTWK8	VF-COMM-01
	VF-COMM-02
	VX-RSI-01
	VX-RSI-02
	VX-RSI-03
	VX-RSI-04
	VX-SPS-01
NTWK14	VC-GEN-02
NTWK15	VC-GEN-02
NTWK16	VC-GEN-02
NTWK17	VC-GEN-02
	VF-COMM-01
	VF-COMM-02
NTWK18	VF-COMM-01
	VF-COMM-08
NTWK20	VF-COMM-01
	VF-COMM-02
NTWK21	VP-MGM-01
NTWK23	VF-COMM-01
	VF-COMM-02
NTWK24	VF-COMM-01
	VF-COMM-02
NTWK27	VF-COMM-04
NTWK28	VC-GEN-02
NTWK31	VF-COMM-01
	VF-COMM-02
NTWK34	VF-COMM-01
	VF-COMM-02
NTWK41	VF-SEC-14
NTWK48	VF-MGM-05
NTWK51	VF-COMM-01
	VF-COMM-02
	VX-ADMU-01
NTWK61	VF-COMM-01
	VF-COMM-02
NTWK75	VF-AMDS-08
	VF-COMM-08
NTWK83	VF-MGM-05
NTWK115	VF-COMM-01

SUBSYSTEM SPECIFICATION ID	NSR SPECIFICATION ID
	VF-COMM-02
NTWK249	VF-MGM-05
NTWK278	VF-COMM-01
	VF-COMM-02
NTWK279	VF-COMM-01
NTWK280	VF-COMM-02
	VF-SEC-04
	VF-SEC-15
NTWK281	VF-SEC-04
	VF-SEC-15
NTWK282	VF-SEC-04
	VF-SEC-15
NTWK283	VF-SEC-04
	VF-SEC-15
NTWK284	VF-SEC-02
	VF-SEC-03
	VF-SEC-14
NTWK285	VF-COMM-07
	VF-SEC-02
	VF-SEC-03
	VF-SEC-04
	VF-SEC-15
NTWK286	VF-COMM-07
	VF-SEC-02
	VF-SEC-15
NTWK287	VF-COMM-07
	VF-SEC-01
	VF-SEC-02
	VF-SEC-03
NTWK288	VF-SEC-02
NTWK289	VF-SEC-14
NTWK290	VF-SEC-14
NTWK292	VF-SEC-14
NTWK294	VF-SEC-01
	VF-SEC-02
NTWK298	VF-SEC-06
	VF-SEC-07
NTWK299	VF-SEC-06
	VF-SEC-07
NTWK300	VF-SEC-07
NTWK301	VF-SEC-07
NTWK302	VF-SEC-07
NTWK303	VF-COMM-07
	VF-SEC-12
NTWK304	VF-SEC-12
	VF-SEC-13
NTWK305	VF-SEC-12

SUBSYSTEM SPECIFICATION ID	NSR SPECIFICATION ID
	VF-SEC-13
NTWK308	VF-SEC-02
	VF-SEC-04
	VF-SEC-15
NTWK309	VF-SEC-15
NTWK311	VF-MGM-05
NTWK312	VF-SEC-14
NTWK313	VF-SEC-14
NTWK314	VP-GEN-01
	VP-GEN-02
NTWK315	VP-GEN-01
	VP-GEN-02
NTWK316	VP-GEN-01
	VP-GEN-02
NTWK317	VP-GEN-01
	VP-GEN-02
NTWK318	VP-GEN-01
	VP-GEN-02
NTWK319	VP-GEN-01
	VP-GEN-02
NTWK320	VP-GEN-01
	VP-GEN-02
NTWK321	VP-GEN-01
	VP-GEN-02
NTWK323	VP-GEN-01
NTWK323	VP-GEN-02
NTWK324	VP-GEN-01
	VP-GEN-02
NTWK327	VF-SEC-12
NTWK328	VF-SEC-12
NTWK332	VF-STS-01
NTWK333	VF-STS-01
NTWK334	VF-MGM-02
NTWK335	VF-MGM-02
	VF-MGM-04
	VF-MGM-05
	VF-MGM-16
NTWK336	VF-MGM-02
	VF-MGM-05
NTWK337	VF-MGM-02
	VF-MGM-05
NTWK338	VF-MGM-03
	VF-MGM-06
	VF-MGM-07
NTWK339	VF-MGM-02
	VF-MGM-09
NTWK340	VF-MGM-13

SUBSYSTEM SPECIFICATION ID	NSR SPECIFICATION ID
	VF-MGM-14
NTWK341	VF-MGM-04
NTWK342	VF-MGM-04
NTWK343	VF-MGM-04
NTWK344	VF-MGM-04
NTWK345	VF-COMM-01
	VF-COMM-02
NTWK346	VF-COMM-01
	VF-COMM-02
	VX-ADMU-01
NTWK347	VF-COMM-01
	VF-COMM-02
NTWK349	VF-COMM-01
	VF-COMM-02
NTWK350	VF-COMM-01
	VF-COMM-02
NTWK351	VF-COMM-01
NTWK351	VF-COMM-02
NTWK352	VF-COMM-01
	VF-COMM-02
NTWK353	VF-COMM-01
	VF-COMM-02
NTWK354	VF-COMM-01
	VF-COMM-02
NTWK356	VF-COMM-01
	VF-COMM-02
NTWK357	VF-COMM-01
	VF-COMM-02
NTWK358	VF-COMM-01
	VF-COMM-02
NTWK360	VF-AMDS-08
	VF-COMM-08
NTWK361	VF-AMDS-08
	VF-COMM-08
NTWK362	VF-AMDS-08
	VF-COMM-08
NTWK363	VF-AMDS-08
	VF-COMM-08
NTWK364	VF-AMDS-08
	VF-COMM-08
NTWK365	VF-AMDS-08
	VF-COMM-08
NTWK366	VF-AMDS-08
	VF-COMM-08
NTWK367	VF-AMDS-08
	VF-COMM-08
NTWK368	VF-AMDS-08

SUBSYSTEM SPECIFICATION ID	NSR SPECIFICATION ID
	VF-COMM-08
NTWK369	VF-AMDS-08
	VF-COMM-08
NTWK370	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK371	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK372	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK373	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK374	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK375	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK376	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK377	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK378	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK379	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK380	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK383	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK427	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK428	VF-COMM-04
	VF-COMM-05
	VF-COMM-06
NTWK429	VF-COMM-04
	VF-COMM-05

SUBSYSTEM SPECIFICATION ID	NSR SPECIFICATION ID
	VF-COMM-06
NTWK452	VF-AMDS-08
	VF-COMM-08